US Army Corps of Engineers ®

U.S. Army Engineering and Support Center, Huntsville

Electronic Technology Systems Center

Technical Bulletin September 2008

On page ...

Visit the U.S. Army Engineering and Support Center, Huntsville at www.hnd.usace.army.mil

A Tribute to Doyce 'Ken' Haynes

By Darrel Anerton
Chief, Electronic Technology Systems Center

For those of us who knew him well, Ken Haynes, was a heck of an engineer, a supportive coworker, but most of all a sincere friend. Ken passed from this life on Aug. 11 – his death was very much unexpected, and he will be sincerely missed as a member of the Corps of Engineers Electronic Security Center (ESC). Ken would have been 62 years old on Aug. 19; he invested 41 years of his life as a Civilian employee of the U.S. Army; and he had been a member of the Corps of Engineers' ESC since 1995.

Ken was an Electronic Security Systems (ESS) technical expert of the highest caliber. During his tenure at the ESC, he provided immeasurable value as a technical expert to a wide spectrum of Army security projects and customers. He was well traveled to our ESC projects that spanned the world in such places as Russia, Bosnia, Iraq, Japan, not to mention all of the Army installations on home soil that he provided service to throughout the years. Ken was recognized in technical circles as an engineer's engineer; he could be counted on to be thorough, meticulous and wise in all the projects he supported. He quickly won the admiration and respect of everyone he came into contact with from day-to-day; his coworkers, contractors and customers all loved him and valued his opinion on ESS technical issues.

Courtesy photo
Doyce K. Haynes

In 2005, Ken was designated as the ESS Mandatory Center of Expertise (MCX) technical deputy and in this role he ensured quality of the products and services delivered by the MCX; he served as a primary interface to our customers; and he lead the MCX team serving as a role model and champion. Ken had a quiet and collected demeanor, and through his leadership he set high standards of performance and integrity for all of us who worked with him. He served with a passion for excellence and a commitment for customer satisfaction that set expectations high for everyone. He was well known, liked and respected as a security professional by his peers across the Army.

Ken will assuredly be missed by all of us here at the Electronic

See *Haynes* on page 5

'Green' your building through proper commissioning

By Will White and Chris Newman

Is your facility as green as it could be? Proper commissioning of your existing heating, ventilating and air conditioning (HVAC) system will go a long way in greening up your part of the world. Systems installed without proper commissioning do not perform as designed, do not save energy and may waste large quantities of energy.

So, what is "commissioning" anyway? Commissioning is simply the process of testing and measuring to ensure the installed equipment is working properly. Generally, there are three designations for this process: commissioning, re-commissioning, and retro-commissioning.

Commissioning on the HVAC equipment and associated controls occurs as a final checkout when a building is first constructed. Optimally, this is achieved before the building is occupied and before government acceptance.

Re-commissioning is the follow-on effort to correct what was missed the first time around. This can occur years later or, in the most egregious circumstances of poor design and workmanship, in only weeks. This will essentially take the equipment and systems back to an "as-built" or "as-installed"/"as-designed" state, just as if the building were being readied for initial occupancy. Usually the occupants will identify the more serious deficiencies and document them through complaints and work requests. Some are not found until engineers test the overall system efficiencies for the HVAC and controls.

Retro-commissioning is reserved for buildings that never received any prior commissioning.

Although there are a lot of advantages to proper commissioning, sometimes it is not followed and enforced. This is due largely to the following common problems or misconceptions:

- Costs. The general thought is that commissioning costs too much or that the return on the investment is too low.
- Education. Usually new construction in the military is managed by civil engineers. Due to their engineering discipline and lack of familiarity, they are less likely to focus on the essential details of mechanical and electrical control systems. The direct digital controls that execute a proper sequence of operations are often misunderstood and not fully tested.
- Lack of Training. There may be insufficient training in the specialized and complicated world of commissioning.
- "Fox in the hen house" issue (the commissioning agent and prime contractor are in collusion). Proper commissioning can only be performed when a totally independent commissioning agent is hired and is only responsible to the building owner, totally outside the financial and direct line of authority of the constructor.
- Enforcement. The design specifications have not been enforced, usually due to lack of training or familiarity with HVAC and control systems.
- Indifference. "The system is working – nobody is complaining" or "It's not my problem."

The good news is that there are testing and balancing contractors and independent commissioning teams available to perform commissioning properly. A good commissioning experience may be achieved with a partnership between the customer and the commissioning team. The key is to write a VERY detailed testing procedure (similar to MIL-STD-2002): "If I push this button, then x starts," etc. The customer/user needs to let the TAB contractor know that a validation process will occur to ensure values are accurate per their submitted report. The TAB contractor will be required to correct all noted deficiencies. The quality assurance process will test the air flow rate on diffusers, variable air volume boxes and air handlers. It will exercise the sequence of operations and ensure all the dampers and valves are correctly positioned. It will ensure that every point is tested, and it will test all analog point calibrations against a traceable (e.g., ANSI) standard.

Our overall goal is to have maintainable buildings and to save energy and money while doing so. You never know what you may find during commissioning testing. There

See *Green* on page 5

Huntsville Center's electronic security system design course offers worldwide training

By Jenny Stripling
Public Affairs Office

In the aftermath of Sept. 11, 2001, a greater emphasis on new technology and higher levels of security for military facilities worldwide has emerged.

Installations are upgrading, and in some cases installing, electronic security systems to support the need for higher levels of security.

The Mandatory Center of Expertise for Electronic Security Systems, located at the U.S. Army Engineering and Support Center, Huntsville, is aiding installations by offering the ESS Design Course as a way to train professionals on the proper selection and application of current, state-of-the-art electronic security equipment and software.

The focus of the design course is to give the participants basic knowledge and skills necessary to contribute to an ESS design.

Instructors of the ESS Design Course begin preparing and planning course material between October and December with actual course sessions running from mid-January through September.

In a typical year, the ESS Design Course offers four sessions at the dedicated ESS training facility located on Redstone Arsenal, Ala., and three sessions at various locations both in the U.S. and overseas. In the past three years mobile training teams have visited Florida, Virginia, Massachusetts and Washington, D.C., as well as Germany, Japan, Korea and Hawaii.

"We usually travel overseas where there is a concentration of U.S. military personnel. If it's a task for them to come here, we go to them," said lead instructor Charles Malone. "The course can also be taken remotely within the U.S., but we strongly encourage students to come to our main training facility at Redstone because it has all the live equipment, classrooms, the whole works. They can actually see the types of systems they are going to be designing."

Each session begins on Monday and ends on Friday for 36 hours of organized classroom instruction. According to Malone, students are not just given lectures on the systems information but a more hands-on approach is taken to ensure adequate training and understanding of electronic security systems.

Courtesy photo

The Electronic Security Systems Design Course trains professionals on the proper selection and application of electronic security equipment and software.

"One week of the program gives our students an understanding of technology and equipment used in electronic security such as card access, video cameras and intrusion detection," Malone said. "They put their knowledge of these security systems to good use by creating an ESS design, deciding what security equipment they should use, how to use it and why."

On the first day of class, students are given a one-page problem statement. Working in six-person design teams, they have to design a system that meets the security objectives without exceeding the budget. Students work on the problem the entire week of training and have to give a group presentation on their design at the culmination of the course week.

Cathy Works, an intern with the Security and Intelligence Branch of Headquarters, U.S. Army Medical Command, attended the course in April. She came into the course not knowing how much she really did not know about electronic security systems.

"I thought the course was very beneficial," Works said. "By the end of the week, I was more knowledgeable on many aspects of electronic security systems and the individual components that comprise various systems. As an intern I am required

See *ESS course* on page 7

Electronic security systems, accreditation at SCI facilities

By Linda Taylor

Sensitive Compartmented Information (SCI) is classified information concerning or derived from intelligence sources, methods or analytical processes and is required to be exclusively handled within a formal control system established by the Director of Central Intelligence (DCI). A SCI Facility (SCIF) is an accredited area, room, group of rooms, building or installation where SCI may be stored, used, discussed and/or electronically processed.

In order for a specific place to be accredited, it must be approved and meet the physical, technical and personnel security standards prescribed in the Director of Central Intelligence Directive (DCID) 6/9 "Physical Security Standard for Sensitive Compartmented Information Facilities".

The accreditation is granted by the Cognizant Security Authority (CSA) for each SCIF. The CSA is the single point of contact designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods under the SOIC responsibility. The SOIC is the head of an agency, office, bureau or intelligence element identified in section 3.4(f) (1-6) of Executive Order 12333 or successor orders, directives or laws.

The SOIC belongs to a group of intelligence elements formerly known as the "Big 5" but now they are the "Big 6". The "Big 6" are the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial-Intelligence Agency, (NGA), the National Reconnaissance Office (NRO) and the recently added Department of Homeland Security (DHS).

The mission and customer of the SCIF determines from which intelligence element the CSA will come from. For example, DIA is responsible for managing all source production efforts of the intelligence organization of the four military services: Air Force, Army, Navy and Marines. It manages the Defense-wide capabilities for human intelligence (HUMINT), measurement and signature intelligence (MASINT), and the Global Defense Communication Network. In most instances, if your customer is one of the four military services and your SCIF performs a HUMINT or MASINT function, your CSA will come from DIA. Your CSA may come from NSA, NRO, NGA or DHS if your SCIF performs a function assigned to those organizations. NSA is responsible for signal intelligence. NRO develops and operates reconnaissance satellites. NGA prepares geospatial data needed for targeting. DHS is responsible for fusing law enforcement and intelligence information related to terrorist threats to the homeland.

Providing an effective Electronic Security System (ESS) for a SCIF begins before construction. This process begins with the design phase by determining who your CSA is and with Annex A, "SCIF Accreditation Checklist", in DCID 6/9. Sometimes, this checklist is also called a Fixed Facility Checklist (FFC). The FFC, because of its content, may be classified. The ESS project engineer should review

See *SCIF* on page 5

The "Big 6" consist of the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office and the recently added Department of Homeland Security.

Green

continued from page 2

may be major construction errors, such as insufficient air flow due to a closed fire damper in a sealed duct with no access panel. Renovations could have changed the area without addressing HVAC. For example a newly added office is always too hot because the VAV box was not relocated and is now attempting to handle several small spaces instead of one large one. One item commonly found during commissioning is VAV boxes configured with an application specific controller with "default" settings and/or minimal attention to setup parameters causing improper operation. For example, a VAV controller is configured for an 850 CFM box. Upon testing, we find the box actually flows 1024 CFM in the full-open damper position, therefore the setup error causes improper damper positioning attempting to satisfy supply air CFM or space temperatures.

As with most things in our business, cost is a major factor of concern. However, commissioning new buildings or major renovations is generally about 1 percent of the construction cost, and many studies show a good return on the investment. But what about older, remodeled buildings? Unfortunately, re-commissioning is much more expensive. Companies that specialize in this segment have shown costs anywhere from 50 cents to 75 cents per square foot. This is compelling reasoning to do commissioning well at the beginning. Still, issues corrected as a result of commissioning could drastically reduce energy usage and costs now, as well as leave a smaller carbon footprint for the future.

For more information on commissioning, please contact the Utility Monitoring and Controls Systems Mandatory Center of Expertise at 256-895-1749.

SCIF

continued from page 4

the FFC, if completed or assisted with the completion of the FFC.

Intrusion Detection Systems (IDS) requirements are outlined in Annex B of DCID 6/9. Compliance is mandatory for SCIFs established after the effective date of the annex. The IDS shall detect attempted or unauthorized human entry into the SCIF. However, in order to provide an effective ESS for any SCIF, one must become familiar with the entire DCID 6/9. For example, Annex F, "Personnel Access Controls" contains the requirements for automated personnel access control systems for SCIFs. SCIF entrances, unless otherwise stated within the DCID 6/9, shall be under visual control to deny unauthorized access unless the SCIF is unoccupied and secured. The Intrusion Detection Equipment (IDE) must comply with Underwriters Laboratory (UL)-2050 or equivalent as approved by the CSA in writing. Hence, the ESS contractor must be UL-2050 certified. Each installed system must be issued a UL-2050 certificate.

Remember, an effective ESS in any SCIF begins with your CSA and your FFC.

Haynes

continued from page 1

Technology Systems Center. We certainly enjoyed sharing time and space with such a fine man. Upon recently returning from a trip to Japan supporting one of his notable customers, the customer's reaction to his death says what is in many of our hearts:

"I grieve because I feel like I have lost more than a colleague; I have lost a brother and a friend. I know anyone who ever worked with him can witness to the same. Ken is irreplaceable as a colleague and friend. He was a consummate professional with the most pleasant smile and classic southern hospitality. He never gave in or compromised his position whenever he was under pressure to do so. My time working with Ken was a blessing, and I am forever grateful for the knowledge, skill and professionalism he brought to work every day. I will truly miss him along with you."

Ken was survived by his wife Dorothy and his two children, Kyle and Kerisa. I would ask that you please remember them in your thoughts and prayers in the days ahead.

And so we say so long to our great friend and colleague.

Enhanced security pedestrian gate tested, fielded

By Jeff Alford

With the increasing costs from employing contract security guard services, the Headquarters Department of the Army, Office of the Provost Marshal General directed the use of electronic access control technologies to the greatest extent possible to reduce the growing costs.

Using commercial-off-the-shelf electronic entry control equipment, the concept of an Enhanced Security Pedestrian Gate was researched, designed, implemented, tested and fielded. The ESPG is an interlocked mantrap designed to provide access to personnel at unmanned gate positions. In addition, it allows all authorized personnel to gain entry and egress from the government installation including disabled personnel, personnel with children and wheelchair-bound personnel who cannot be accommodated using traditional turnstiles.

Courtesy photo

This Enhanced Security Pedestrian Gate, an interlocked mantrap designed to provide access to personnel at unmanned gate positions, is being used in Weisbaden, Germany.

The ESPG is designed to reduce the requirement for contract security guards as well as detect, deter and prevent unauthorized personnel from entering the installation using a lost or stolen identification card. The ESPG uses an automated entry control process allowing individuals enrolled in the Defense Biometric Information System/Installation Access Control System to obtain access to the installation through the ESPG using an automated verification concept.

By using the DBIDS/IACS as the ESPG's access database, the ESPG validates authorized ID cardholders for entry onto the installation. The installation access process is initiated when the cardholder slides his/her ID card through the card reader slot. At this point, the ESPG communicates with the DBIDS/IACS database to determine if the individual is enrolled in DBIDS/IACS and authorized on that installation. Upon confirmation, the ESPG unlocks the outer door for the cardholder to enter into the ESPG. While entering through the outer doorway, the ESPG scans for multiple persons who may be attempting to enter.

Once the outer door is closed, the cardholder places his/her index finger on the biometric reader where the fingerprint is scanned. The ESPG then communicates with the DBIDS/IACS database which compares the scanned fingerprint to the fingerprint image on record of the user's ID card. Upon confirmation of a match, the inside door will open allowing the cardholder access onto the installation.

There are conditions that will halt the access process, such as: a) the person is not enrolled in DBIDS/IACS, b) the person is either barred or not authorized to enter the installation, c) multiple persons are detected attempting to enter the installation at the same time, d) the fingerprint presented does not match the card swiped to enter the ESPG, or e) the fingerprint reader could not successfully read the print presented. This is usually caused by improper seating of the finger on the biometric reader.

Key operational features include:

1. The ESPG is under continuous surveillance by a closed circuit television system that is continuously recording.
2. Cameras are used to observe persons approaching, using and exiting the ESPG.
3. Only the provost marshal or other designated security officials will have access to downloading or performing administrator functions on the monitoring/recording system. The recording systems employed as part of the total monitoring system have a recording and retrieval capability of up to approximately 30 days. After a maximum of 30 days, the recorded images will be overwritten by images recorded during the next 30-day recording cycle. The capability to download the recording to a writable compact disk does exist.

The ESPG is equipped with guard-override capability to allow valid ID cardholders to access the installation without the cardholder having to present a fingerprint or if the cardholder is handicapped, wheelchair-bound or accompanied by unregistered family members.

See *ESPG* on page 7

ETSC Bulletin needs your input

Beginning Spring 2009, the ETSC Bulletin will have a new section to promote more community-wide idea sharing. We're calling the new section the "View From The Field" and are soliciting ideas, abstracts and even articles from our eyes-on-the-ground – YOU! If there are problems with your ESS or UMCS system that you're facing at your site or if you've found a neat solution to that frustrating issue, chances are there are others just like you who have the same issues. We want to help spread the word on current events happening from YOUR point of view. Please submit your ideas, abstracts and articles to us via email at Contact-ESC@usace.army.mil. We look forward to hearing from you and thank you for your help!

ESS course

continued from page 3

to attend various security-related courses and training sessions. This is one of the most interesting courses I've taken in the past seven months."

To find out more information about upcoming sessions or to register for the courses, e-mail Contact-ESC@usace.army.mil.

In addition to the ESS Design Course, the Huntsville Center's Electronic Security Center also leads training in the Integrated Commercial Intrusion Detection Systems Operator Training Course and the ICIDS III System Administrator Training Course, both offered at a state-of-the-art facility on Redstone Arsenal.

Recently the classes offered have been a combination of the ICIDS Operator Training the first half of the week and ICIDS III System Administrator Course the last half to avoid the inconvenience of expenses and travel.

The two ICIDS courses go hand-in-hand, one building on top of the other.

ICIDS are in place or installed at various government installations and facilities, so through the Operator Training, students learn how to operate a variety of intrusion detections systems, alarms, etc., and how the ICIDS operates in conjunction with these.

The second half of the week students attend the ICIDS III System Administrator Course, designed to provide them with the skills required to successfully operate and manage a functional ICIDS III, either already in place or being installed at various government installations.

All training course calendars and information can be found online at https://eko.usace.army.mil/training/icids_training.

ESPG

continued from page 6

Entry through the outer doorway with a swiped ID card is required and the guard can verify the cardholder has installation access privileges via comparing the image displayed on the DBIDS/IACS laptop with the images from CCTV video system.

The ESPG is equipped with an intercom system. Any individual may contact the ESPG guard monitoring station and request assistance or notify them of an emergency. If primary power is lost, there is a four-hour backup supply so the ESPG will continue working. The door that opens to the inside of the installation remains locked.

The ESPG is equipped with duress, fire and multiple person/presence detection alarms which annunciate at the ESPG guard monitoring station. In the event of a fire alarm, the system will go into fail-safe mode releasing the door that opens to the outside of the installation allowing the person to exit the ESPG and move away from the installation. Mounted on the ceiling and walls are presence detectors designed to detect the presence of multiple persons. If activated, the access process will halt and an alarm will be generated at the guard monitoring station. If someone falls or appears unconscious, the presence detector will signal an alarm to the guards. The guards have a remote Key Switch to open the outer door to provide assistance.

U.S. Army Engineering and
Support Center, Huntsville
4820 University Square
Huntsville, AL 35816-1822

Phone: 256-895-1740
DSN: 760-1740
Fax: 256-895-1519

Check us out online:

ESC

www.hnd.usace.army.mil/esc

- **History of the ESC**
- **Why choose the ESC?**
- **List of clients**
- **Services offered**

UMCS

www.hnd.usace.army.mil/umcs

- **What does UMCS offer?**
- **Why choose UMCS?**

Useful Acronyms:

ACP: Access Control Point

ESC: Electronic Security Center

ESS: Electronic Security Systems

ETSC: Electronic Technology Systems Center

MCX: Mandatory Center of Expertise

UMCS: Utility Monitoring and Controls Systems

ASK MCX!

Q: What procedures should I follow to test my newly installed ESS or UMCS?

A: After installation is complete, the contractor should edit "generic" government-provided procedures to address a site-specific ESS or UMCS configuration. The contractor will submit performance verification test (PVT) procedures to the government for review/ approval prior to testing. Testing of a new system is extremely important. Successful PVT completion is usually a major milestone for the contractor and ensures that the system is ready for operational use.

Who We Are

The Electronic Technology Systems Center (ETSC) is a team within the U.S. Army Corps of Engineers that provides unmatched experience and technical expertise in the specialized fields of Utility Monitoring and Control Systems (UMCS) and Electronic Security Systems (ESS).

Located in Huntsville, Ala., the ETSC supports the Corps of Engineers, the Army, other services and various defense and federal agencies. ETSC has hundreds of active projects around the world.

In its technical consulting role, the ETSC performs engineering surveys, develops criteria, reviews designs and conducts special studies and training for a wide variety of customers. For those customers needing "turn-key" project execution, the ETSC provides indefinite delivery, indefinite quantity (ID/IQ) contracts for system engineering, procurement and installation through a seamless, expedited task order process.

Each year the ETSC participates in numerous conferences, symposia, working groups and trade shows to build relationships and influence future development and application of UMCS and ESS technology.

Contact — esc@usace.army.mil or call 256-895-1740